

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA

NETWORK PROTECTION SCIENCES,  
LLC,

Plaintiff,

v.

FORTINET, INC.,

Defendant.

No. C 12-01106 WHA

**TENTATIVE CLAIM  
CONSTRUCTION ORDER,  
REQUEST FOR CRITIQUE  
AND ORDER STRIKING  
REPLY MATERIALS IN PART**

**INTRODUCTION**

In this patent infringement action involving network firewalls, the parties seek construction of six phrases found in the asserted patent. Those phrases are construed below. This order also **GRANTS IN PART AND DENIES IN PART** Fortinet's motion to strike portions of plaintiff's reply claim construction brief.

Each side has until **NOON ON JANUARY 2, 2012**, to submit a five-page critique (double-spaced, 12-point Times New Roman font, no footnotes, and no attachments) limited to points of critical concern regarding claim construction only. This is an opportunity for the parties to focus solely on their most cogent critique, not to rehash every point made in the briefs and at the hearing.

**STATEMENT**

The technology described in United States Patent No. 5,623,601 dates to 1994. Although the modern internet was still unknown to large sections of the general public at the time,

1 networked computing had been around for decades. Computer viruses and other network  
2 security threats were already a problem of substantial concern. Computer firewalls — network  
3 barriers that analyze packets of information to determine whether they should be let through —  
4 were a relatively recent response to these threats. The technology at issue in this action relates to  
5 firewall technology intended to improve network security and user convenience.

6 Plaintiff Network Protection Sciences (“NPS”) is asserting 54 of the 59 claims in the  
7 ’601 patent against defendant Fortinet, Inc. The parties seek construction of six phrases  
8 appearing in this patent. Fortinet also moves to strike two items of evidence cited in NPS’ reply  
9 claim construction brief. This order begins by addressing Fortinet’s motion to strike; overviews  
10 of the patents, the disputed phrases, and the associated claim are covered in detail afterward.

#### 11 ANALYSIS

##### 12 1. FORTINET’S MOTION TO STRIKE.

13 The parties disagree over the proper construction of the Patent Local Rules. Patent Local  
14 Rule 4-2(b) requires that the parties “identify all references from the specification or prosecution  
15 history that support its proposed construction and designate any supporting extrinsic evidence”  
16 at the same time they exchange preliminary claim constructions. For the joint claim construction  
17 statement, Patent Local Rule 4-3(b) requires that each party identify “any extrinsic evidence  
18 known to the party on which it intends to rely either to support its proposed construction or to  
19 oppose any other party’s proposed construction.” For claim construction briefs, Patent Local  
20 Rule 4-5 requires that the parties serve and file “any evidence supporting . . . claim construction”  
21 along with the opening briefs, and “any evidence directly rebutting the supporting evidence”  
22 with the reply briefs.

23 NPS contends that Patent Local Rule 4-5 allows a party to submit new evidence in a  
24 reply claim construction brief for rebuttal purposes. Fortinet contends that Patent Local Rules 4-  
25 2(b) and 4-3(b) preclude doing so. The parties have identified decisions in this district that are  
26 inconsistent. *Compare Nordic Naturals, Inc. v. J.R. Carlson Labs., Inc.*, No. 7-2385, 2008 WL  
27 2357312, at \*11 (N.D. Cal. June 6, 2008) (Judge Hamilton) (striking a declaration filed with an  
28 opposition claim construction brief), *with Competitive Techs. v. Fujitsu Ltd.*, 286 F. Supp. 2d

1 1161, 1169 (N.D. Cal. 2003) (Magistrate Judge Spero) (refusing to strike a declaration because  
2 Patent Local Rule 4-5 “expressly permits” rebuttal testimony).

3 Our local rules aside, Federal Rule 12(f) addresses a more fundamental concern —  
4 relevance — and allows a court to strike any “immaterial” matter from a pleading. Fortinet first  
5 objects to Exhibit M from NPS’ claim construction reply, which is a 2005 press release from the  
6 website “gpl-violations.org” claiming that certain Fortinet products use a Linux operating system  
7 kernel. NPS candidly admits that the exhibit is not relevant to claim construction. Nevertheless,  
8 NPS wishes to use this exhibit to rebut Fortinet’s attempt to limit the invention to a UNIX  
9 system and to “cast UNIX as an outdated, obsolete operating system” (Dkt. No. 174).

10 It is clear that Fortinet’s alleged use of Linux in 2005 has no bearing on NPS’s 1994  
11 patent. Although Fortinet calls the claimed invention “obsolete,” Fortinet clarifies in its reply to  
12 the motion to strike that it is not arguing that UNIX itself is outmoded (Dkt. No. 182). Fortinet  
13 will be held to this representation and Exhibit M to NPS’ claim construction reply shall be  
14 deemed **STRICKEN**.

15 Fortinet also objects to Exhibit O from NPS’ claim construction reply, which is a  
16 collection of statements *by Fortinet* during *ex parte* reexamination regarding the construction of  
17 the term “transparently.” NPS argues that these statements will help the Court construe the term  
18 in the instant action. Fortinet claims that its own statements during reexamination are irrelevant.  
19 On this point, Fortinet is incorrect.

20 During reexamination, Fortinet asserted that “transparently” meant “not requiring the  
21 user to log in to the firewall.” In this proceeding, an element of NPS’ proposed construction is  
22 the absence of “extra procedures” to accomplish communications, and NPS contends that an  
23 example of an extra procedure would be logging into a firewall. Fortinet asserts that NPS’  
24 construction here is an “audacious attempt” redefining the term “transparently,” and that it  
25 “makes no sense” (Dkt. No. 171 at 18, 20).

26 Fortinet’s position on this term during reexamination and its position here conflict  
27 sharply. Exhibit O is therefore relevant to the credibility of the current argument by Fortinet and  
28 the weight that it should be accorded.

1 As to whether the exhibit was untimely submitted under our local rules, NPS was or  
2 should have been aware that Fortinet was taking a conflicting position on the term  
3 “transparently” when the parties submitted their joint claim construction statement (Dkt. No.  
4 166). Under Patent Local Rule 4-3(b), NPS should have identified “extrinsic evidence . . . on  
5 which it intends to rely . . . to oppose any other party’s proposed construction.” NPS cannot  
6 argue that it should be exempted from the rule. Although the intensity of Fortinet’s rhetoric may  
7 have been unexpected, NPS cannot (and does not) argue that it only learned during the claim  
8 construction briefing that Fortinet would contradict its prior position. On the other hand, the  
9 rationale behind this rule is to prevent one party from catching the other off guard with new,  
10 surprise evidence. Fortinet cannot be surprised by its own statements to the PTO. This order  
11 finds that the rationale for enforcing the local rule is not met in these particular circumstances.  
12 Fortinet’s motion to strike Exhibit O is **DENIED**.

13 Because Exhibit M has been stricken, Fortinet’s request for a sur-reply on that issue is  
14 **MOOT**. Fortinet had an adequate opportunity to address the issue of its prior statements during  
15 oral argument, so further briefing regarding Exhibit O is unnecessary. It is also unnecessary to  
16 address NPS’ contention that Fortinet failed to timely disclose evidence because NPS does not  
17 request any resulting relief.

## 18 2. CLAIM CONSTRUCTION LEGAL STANDARD.

19 Claim construction is from the perspective of one of ordinary skill in the pertinent art at  
20 the time the patent was filed. *Chamberlain Group, Inc. v. Lear Corp.*, 516 F.3d 1331, 1335  
21 (Fed. Cir. 2008). While claim terms “are generally given their ordinary and customary  
22 meaning,” the “claims themselves provide substantial guidance as to the meaning of particular  
23 claim terms.” As such, other claims of the patent can be “valuable sources of enlightenment as  
24 to the meaning of a claim term.”

25 Critically, a patent’s specification “is always highly relevant to the claim construction  
26 analysis.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–15 (Fed. Cir. 2005) (en banc) (internal  
27 quotations omitted). Indeed, claims “must be read in view of the specification, of which they are  
28 a part.” *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc),

1 *aff'd*, 517 U.S. 370 (1996). Finally, courts also should consider the patent's prosecution history,  
2 which "can often inform the meaning of the claim language by demonstrating how the inventor  
3 understood the invention and whether the inventor limited the invention in the course of  
4 prosecution, making the claim scope narrower than it would otherwise be." These components  
5 of the intrinsic record are the primary resources in properly construing claim terms. Although  
6 courts have discretion to consider extrinsic evidence, including dictionaries, scientific treatises,  
7 and testimony from experts and inventors, such evidence is "less significant than the intrinsic  
8 record in determining the legally operative meaning of claim language." *Phillips*, 415 F.3d at  
9 1317–18 (internal quotations omitted).

10 While this order acknowledges that the parties have a right to the construction of all  
11 disputed and litigated claim terms by the time the jury instructions are settled, the Court will  
12 reserve the authority, on its own motion, to modify the constructions in this order if further  
13 evidence — intrinsic or extrinsic — warrants such a modification. Given that claim construction  
14 is not a purely legal matter, but is (as the Supreme Court describes it) a "mongrel practice" with  
15 "evidentiary underpinnings," it is entirely appropriate for the Court to adjust its construction of  
16 claims prior to instructing the jury if the evidence compels an alternative construction, or if one  
17 side or the other advances a spin on the words that is unwarranted. *Markman*, 517 U.S. at 378,  
18 390. The parties should be aware, however, that they are not invited to ask for reconsideration of  
19 the constructions herein. Motions for reconsideration may be made only in strict accordance  
20 with the rules of procedure, if at all.

### 21 3. THE '601 PATENT.

22 The '601 Patent, entitled "Apparatus and Method for Providing a Secure Gateway for  
23 Communication and Data Exchanges Between Networks," was filed on November 21, 1994, and  
24 issued on April 22, 1997. Milkway Networks Corporation is the assignee, and plaintiff is  
25 Milkway's successor-in-interest. In 2011, Fortinet filed a request for reexamination, and in May,  
26 2012 the USPTO issued a reexamination certificate for the patent confirming all claims (1–41)  
27 and adding new claims (42–59).  
28

In this action, NPS is asserting 54 of the 59 claims in the '601 patent, including both method and apparatus claims. The six claim terms for which the parties seek constructions can be found, *inter alia*, in claims 1, 10, and 11 (reproduced below with the relevant claim terms italicized).

Claim 1 covers the following method (col. 14:11–42):

1. A method of providing a secure gateway between a private network and a potentially hostile network, comprising the steps of:
  - (a) addressing communications packets directly to a host on the potentially hostile network as if there were a communications path to the host, but encapsulating [*sic*] the packets with a hardware destination address that matches a device address of the gateway;
  - (b) *accepting at the gateway* communications packets from either network that are encapsulated with a hardware destination address which matches the device address of the gateway;
  - (c) determining at the gateway whether there is a *process bound to a destination port number* of an accepted communications packet;
  - (d) establishing *transparently* at the gateway a first communications session with a source address/source port of the accepted communications packet if there is a *process bound to the destination port number*, else dropping the packet;
  - (e) establishing *transparently* at the gateway a second communications session with a destination address/destination port of the accepted communications packet if a first communications session is established; and
  - (f) *transparently* moving data associated with each subsequent communications packet between the respective first and second communications sessions, whereby the first session communicates with the source and the second session communicates with the destination using the data moved between the first and second sessions.

Claim 10 covers the following method (cols. 15:45–16:14):

10. A method of providing a secure gateway between a private network and a potentially hostile network, comprising the steps of:
  - (a) addressing communications packets directly to a host on the potentially hostile network as if there were a communications path to the host, but encapsulating [*sic*] the packets with a hardware destination address that matches a device address of the gateway;
  - (b) accepting from either network all TCP/IP packets that are encapsulated with a hardware destination address which matches the device address of the gateway;

- (c) determining whether there is a *proxy process* bound to a port for serving a destination port number of an accepted TCP/IP packet;
- (d) establishing a first communications *session* with a source address/source port number of the accepted TCP/IP packet if there is [*sic*] *proxy process* bound to the port for serving the destination port number, else dropping the packet;
- (e) determining if the source address/source port number of the accepted packet is permitted to communicate with a destination address/destination port number of the accepted packet by referencing a rule base, and dropping the packet if a permission rule cannot be located;
- (f) establishing a second communications *session* with the destination address/destination port number of the accepted TCP/IP packet if a first communications *session* is established and the permission rule is located; and
- (g) *transparently* moving data associated with each subsequent TCP/IP packet between the respective first and second communications *sessions*, whereby the first *session* communicates with the source and the *second* session communicates with the destination using the data moved between the first and second *sessions*.

Dependent claim 11 covers the following method (col. 16:15–23):

11. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 10 wherein the step of determining involves checking a table to determine if a custom *proxy process* is *bound to the destination port number*, and passing the packet to a *generic proxy process* if a custom *proxy process* is *not bound to the destination port number*, the *generic proxy process* being executed to establish the first and second communications *sessions* and to move the data between the first and second communications *sessions*.

The patent addresses a basic concern created by the existence of public and private computer networks. Private networks, such as single corporation's intranet, are relatively secure, and often store trade secret and confidential information that must be shielded from public exposure. Public networks, such as the internet, are accessible to anyone with the right hardware and software, and as a consequence attract sabotage, vandalism, and espionage. When a private network connects to a public network, it becomes exposed to these threats. To deal with the problem, secure gateways are installed between the networks to serve as "firewalls" (col. 1:23–40).

At the time of the invention, firewalls suffered from known disadvantages that compromised their security or inconvenienced users. One firewall technology in the prior art



1 was the “packet filter.” Packet filters were (and are) host-based applications that permitted  
2 certain kinds of communications over predefined ports and use pre-defined rule sets to determine  
3 what information to let through. Because an operating system such as UNIX running TCP/IP  
4 (the communication protocol for the internet) could have 64K communication ports, it was  
5 considered impractical to maintain a comprehensive rule base (col. 2:35–45).

6 Another firewall technology, “dual homed gateways,” blocked direct traffic and required  
7 the public and private networks to each communicate with the gateway. When implemented at  
8 the application level, users could (and can) only access specific public services allowed by the  
9 gateway. These application level firewalls, however, were inefficient because they generally  
10 required the user to execute time-consuming extra operations or to use specially-adapted  
11 network-service programs (col. 3:4–22). Also, application level firewalls required application  
12 interfaces for each public network service, and did not support applications using dynamic port  
13 allocations assigned in real time (col. 3:48–52).

14 The claimed invention allegedly overcame these problems by modifying a secure  
15 gateway station to accept all IP packets with a certain encapsulation. The invention provided for  
16 communication sessions to be initiated between (i) the source network (the network sending the  
17 packet) and (ii) the destination network (the network receiving the packet). The “payload” data  
18 in the packet were then passed between the two sessions. The new process was more efficient  
19 for the user because from the user’s perspective the information was passed as if no gateway  
20 existed. The invention also provided for a generic proxy process to handle data such that the  
21 gateway could use all 64K ports available on a UNIX operating system and could support  
22 dynamic port allocation (cols. 4:17–5:55).

23 **A. “Session”**

24 The parties dispute the term “session.” Both provide constructions, but NPS argues that  
25 “session” is a term of art that preferably should be given its ordinary meaning. The parties’  
26 proposed constructions are provided below:  
27  
28



## NPS' PROPOSED CONSTRUCTION

FORTINET'S PROPOSED  
CONSTRUCTION

Plain and ordinary meaning; or

A connection between two functional units, such as two terminals, stations, or computers, that allows them to communicate for a period of time or a logical association that is established and maintained between two functional units that allows them to communicate.

The application level network gateway and source maintain a connection and transfer information, or the application level network gateway and destination maintain a connection and transfer information

This order concludes that the plain and ordinary meaning of the term “session” should govern, as understood by one of ordinary skill in the art in 1994.

NPS' proposed alternative construction for “session” is turgid and unhelpful. Its proposal to use the ordinary meaning fares better. NPS does not provide much explanation for its argument that the term should given its ordinary meaning. Nevertheless, it was a straightforward term in 1994 (and today).

Fortinet's only challenge to using the ordinary meaning of the term “session” is that the patent “always” referred to a session as including the transfer of information. Fortinet's assertion is incorrect. Information *could* be transferred during a session, for example by a proxy process or by the kernel (the program at the core of the computer operating system that supported programs running at the application level). The specification also disclosed a situation where a proxy process handling communications would not transfer information. The proxy process could determine that a session had not ended and could wait for data packets to arrive (col. 11:56–65). If a proxy process could wait for data to arrive during an active session but without transferring data, it is clear that a session did not necessarily require information transfer.

This order concludes that the plain and ordinary meaning of the term “session” should govern (subject to a possible refinement after the trial evidence is heard).

**B. “Proxy process”**

The parties dispute the term “proxy process.” The parties’ proposed constructions are provided below:

NPS’ PROPOSED CONSTRUCTION	FORTINET’S PROPOSED CONSTRUCTION
An application layer process adapted to handle a respective service.	A program running on an application level network gateway that initiates the first session and second session, and relays “the data portion of each packet” between the sessions.
or (at oral argument):	
An application layer process adapted to handle communications across a gateway for a respective service	

This order finds that the term should be construed as: “an application layer process adapted to handle communications for a network service.”

The term “proxy” was defined in the patent specification. To wit:

When the gateway station 14 is initialized, a system configuration file is examined to determine what network services are to be supported by the gateway station 14. In order to maximize performance efficiency of the gateway station 14, commonly used services are supported by processes adapted to most efficiently handle communications for each respective service. These processes are called “proxies.”

(Col. 9:47–54.) NPS’ proposed constructions are reworded versions of this definition. Fortinet asserts that it is improper to rely on an isolated passage of the specification in support of a broad construction. Fortinet’s attempt to define the patent differently than it was defined by the patentee himself is unpersuasive.

Fortinet asserts that NPS’ proposed construction is an attempt to scrub the patent of its reliance on a “proxy concept,” and that the term should be construed to require a process that “actually acts as a proxy.” At oral argument, Fortinet explained that the patent should be viewed through a particular technological lens — what Fortinet refers to as a “proxy everything” environment. This is an attempt to limit the scope of the claims generally by creating a limiting context. Otherwise, Fortinet contends, NPS’ definition could be read to include any process, even processes that are not proxies.

Fortinet’s desire to ignore the definition in the specification is improper. “It is a well-established axiom in patent law that a patentee is free to be his or her own lexicographer,

1 and thus may use terms in a manner contrary to or inconsistent with one or more of their  
2 ordinary meanings.” *Hormone Research Found., Inc. v. Genentech, Inc.*, 904 F.2d 1558, 1563  
3 (Fed. Cir. 1990) (citation omitted). “When a patentee explicitly defines a claim term in the  
4 patent specification, the patentee’s definition controls.” *Martek Biosciences Corp. v. Nutrinova,*  
5 *Inc.*, 579 F.3d 1363, 1380 (Fed. Cir. 2009).

6       Aside from this general principle of patent claim construction, the specific limitations  
7 requested by Fortinet are unwarranted. Fortinet asserts that the term proxy process should be  
8 limited to include (i) the concept of relaying a data packet between communication sessions, and  
9 (ii) the concept that the proxy process initiated the communication sessions. NPS agrees that a  
10 proxy process could relay data, but does not agree that it should be so limited. In support, NPS  
11 cites examples in the specification where a proxy process did something else, such as verifying  
12 an IP address. Fortinet’s limitation, therefore, goes to far. The Court’s construction — “an  
13 application layer process adapted to handle communications for a network service” — is more  
14 suitable because these other activities are within the general scope of “handling  
15 communications.”

16       As for whether the proxy process initiated the communication session, Fortinet concedes  
17 that NPS cites examples from the specification where the gateway or kernel initiated the  
18 communications. Fortinet contends that these examples are ambiguous. This order disagrees. In  
19 particular, Figure 6, which was a “flow diagram of . . . TCP routing by a modified UNIX kernel  
20 in accordance with the invention” (col. 6:65–67), showed that the kernel started a session with a  
21 source prior to delivering a packet to a proxy process. The fact that elsewhere in the patent the  
22 proxy process initiated the communication session only demonstrates that both ideas were  
23 disclosed.

24       Another objection by Fortinet in its papers points out a flaw in NPS’ original proposed  
25 construction. A close comparison of the definition in the specification and NPS’ proposed  
26 construction reveals that NPS has omitted the concept of handling communications. This  
27 omission unjustifiably broadens the scope of the claim language, and is easily corrected. At oral  
28 argument, NPS conceded this point by offering compromise construction that included the

concept of communications. In order to align the construction with the definition, this order specifies that the proxy process handles “communications for a network service.”

The full construction of “proxy process” therefore shall read: “an application layer process adapted to handle communications for a network service.”

**C. “Generic proxy process”**

During briefing and oral argument, the parties modified and narrowed their differences over this term, but they still dispute the term “generic” as it modifies the term “proxy process.” The parties’ current proposed constructions are shown below:

NPS’ PROPOSED CONSTRUCTION	FORTINET’S PROPOSED CONSTRUCTION
A process which can handle a service for which a dedicated or custom proxy process is not running.	A proxy process that serves any application not already served by a dedicated custom proxy process.
or (at oral argument):	
A proxy process which can handle a service for which a dedicated custom proxy process is not running.	
or:	
A “proxy process” that serves any service not already served by a dedicated or “custom” proxy process.	

This order construes “generic proxy process” as “a proxy process which can handle communications for a network service for which a dedicated or custom proxy process is not running.”

Aside from the underlying disagreement over “proxy process,” one aspect of the parties’ dispute over this term is whether the terms “dedicated” and “custom” should be listed in the conjunctive or the disjunctive. The specification referred to the generic proxy process operating wherever there was not a “dedicated proxy process” (col. 5:48–52). It is also clear from the specification that the inventor anticipated that a generic proxy process could support a network service until a new, custom proxy processes was written (col. 12:52–55). Thus, the invention conceived of at least three proxy scenarios: a dedicated proxy, a generic proxy, and a custom

1 proxy that displaced a generic proxy already in use. Fortinet's construction in the conjunctive  
2 cannot accommodate all three possibilities, and is therefore too narrow. This order will use the  
3 disjunctive phrasing "dedicated or custom."

4 The other significant distinction between the proposed constructions lies in the gap  
5 between "handle a service" and "serves any application." Here, Fortinet's proposed construction  
6 strays too far afield from the definition of proxy provided by the inventor, and the phrase "serves  
7 any application" is ambiguous.

8 A "generic proxy process" was a specific type of "proxy process." Once again, NPS'  
9 construction strays from the definition of "proxy process" in the specification. For clarity and  
10 consistency, this order will rely on the inventor's definition.

11 In sum, a "generic proxy process" shall be construed to mean "a proxy process which can  
12 handle communications for a network service for which a dedicated or custom proxy process is  
13 not running."

14 **D. "Process bound to a destination port number"**

15 During briefing, Fortinet modified its proposed construction of this term, but the parties  
16 still dispute "process bound to a destination port number." The parties' latest proposed  
17 constructions are shown below:

NPS' PROPOSED CONSTRUCTION	FORTINET'S PROPOSED CONSTRUCTION
Plain and ordinary meaning; or Process assigned or linked to a destination port number.	Proxy process that is bound to the port on the gateway that matches the destination port number of the incoming packets.
	or:  Proxy process bound to a destination port.

22  
23  
24  
25 This order construes "process bound to a destination port number" as meaning a "process  
26 assigned to a destination port number."

27 The parties do not appear to dispute the "destination port number" component of the  
28 term, and the parties did not address the issue in their briefs or at oral argument. Fortinet

nevertheless provides an proposed construction for this element. Fortinet’s construction defines “destination port number” as “the port on the gateway that matches the destination port number of the incoming packets.” Compared with a plain meaning construction, Fortinet’s proposal for this segment is wordy and potentially confusing. Fortinet also does not explain in why explication of “destination port number” is necessary.

The parties’ dispute involves two issues. *First*, they dispute whether “process” must be construed to refer to a “proxy process.” This is the focus of the parties’ dispute over this term, both in the briefing and at oral argument. Here, Fortinet again offers its unsubstantiated contention that the patent taught a “proxy everything” environment. Fortinet further contends that the intrinsic evidence shows that “process bound” always meant a “proxy process.”

What Fortinet’s contentions do not account for is how the term was actually used in the claims. The disputed term appeared in claim 1 in the following clauses:

(c) determining at the gateway whether there is a ***process bound to a destination port number*** of an accepted communications packet

(d) establishing transparently at the gateway a first communications session with a source address/source port of the accepted communications packet if there is a ***process bound to the destination port number***, else dropping the packet;

(Col. 14:23–29 (emphasis added).) In claim 10, the term was used differently:

(c) determining whether there is a ***proxy process bound to a port for serving a destination port number*** of an accepted TCP/IP packet;

(d) establishing a first communications session with a source address/source port number of the accepted TCP/IP packet if there is [*sic*] ***proxy process bound to the port for serving the destination port number***, else dropping the packet;

(Col. 15:56–64 (emphasis added).) In claim 11, there was another variation.

11. A method . . . as claimed in claim 10 wherein the step of determining involves checking a table to determine if a ***custom proxy process is bound to the destination port number***, and passing the packet to a generic proxy process if a ***custom proxy process is not bound to the destination port number*** . . . .

(Col. 16:15–20 (emphasis added).) The reader will note the progression: a “process” was claimed in claim one, but a “proxy process” and a *specific type* of “proxy process” appeared in claims 10 and 11, respectively. It seems clear that the drafter intended to refer to different types

1 of processes being bound. Fortinet’s construction of the disputed term to mean “proxy process”  
2 in claim one would therefore require reading a limitation from the specification into the claims,  
3 or limiting a broader claim based on subsequent narrower claims. This would be improper.  
4 Fortinet’s construction would also render the language in claims 10 and 11 that specifies a  
5 “proxy process” superfluous.

6 *Second*, the parties dispute the meaning of the word “bound.” Fortinet asserts that bound  
7 should be understood to refer specifically to the UNIX “bind” command but does not propose to  
8 include that limitation in the construction. Instead, Fortinet asserts that a POSA would have  
9 considered the ordinary meaning of the term bound to mean the bind command.

10 It is useful to note at this point that Fortinet’s assumption of a UNIX environment is  
11 faulty. It is true that the patent used UNIX to describe an embodiment of the patent (*see* cols.  
12 9:41–10:24). However, the claims of the patent were not limited to the UNIX operating system.  
13 For example, claim 19 described an apparatus that included “*an operating system* executable by  
14 the gateway station, a kernel of the operating system having been modified . . .” (col:17:41–50  
15 (emphasis added)). Claim 20, which was dependent on claim 19, covered an apparatus “wherein  
16 the operating system [was] a Unix operating system” (col. 18:9–12).

17 NPS also wishes to use the ordinary meaning of the term “bound,” but disagrees that it  
18 must include the UNIX bind command. NPS offers “assigned or linked” as an alternative  
19 meaning for “bound.” NPS cites several places in the specification where the term “assigned” is  
20 used in relation to the concept of something being “bound,” but does not cite and support in the  
21 specification for “linked.”

22 This order concludes that only the word “bound” in the disputed term requires a  
23 construction. Helpfully, the patent itself provided a definition:

24 On system initialization, any proxy given operating rights by the system  
25 administrator is said to “bind” to the port to which the proxy has been  
assigned. Thereafter, the process is said to be “bound” to the port.

26 (Col. 9:54–57.) Fortinet argues that this was not a definition, but rather a factual description of a  
27 series of events: the system initialized, and then a process assigned to a port was subsequently  
28 bound in the sense of the UNIX “bind” command. This reading is not justified from the plain



language of the patent, and is premised on Fortinet’s unduly narrow assumption that the patent required a UNIX environment.

The use of the term “assigned” to explain “bound” is evident. “Linked” is not. Accordingly, this order adopts a modified version of NPS’s construction: “process bound to a destination port number” should be construed as meaning a “process assigned to a destination port number.”

#### **E. “Transparently”**

The parties dispute the term “transparently.” The parties’ proposed constructions are shown below:

NPS’ PROPOSED CONSTRUCTION	FORTINET’S PROPOSED CONSTRUCTION
Such that clients on networks can run network service applications without extra procedures or modifications to accomplish communications across a gateway.	Appearing to the initiator to be one direct communications session.

This order adopts Fortinet’s proposed construction of “transparently”: “appearing to the initiator to be one direct communications session.” Fortinet cites multiple instances in the patent specification and in the declaration of NPS’ expert during reexamination where “transparently” was defined in this manner or explained in terms of whether the communications session appears to be direct.

NPS objects on several grounds, none of which are persuasive. *First*, NPS argues that this construction is improper because it defines the term with a description of the subjective result of the claimed method. NPS cites *West v. Quality Gold, Inc.*, No. 10-3124, slip op. at 9–10 (N.D. Cal. Sept. 16, 2011) (Judge Jeremy Fogel), for the proposition that claims should not be defined by the subjective opinion of an individual practicing an invention. NPS’s reliance on *West* is misplaced. NPS conflates subjective opinion with a subjective experience of an objective fact. Unlike the phrase “pleasing appearance” in *West*, “transparency” in Fortinet’s proposed construction does not require a subjective evaluation. Whether a communication session appears to be direct is only based on whether there is an objectively perceptible

intermediary. An intermediary either appears and is perceived by the client, or it does not. This does not require a subjective opinion.

*Second*, NPS asserts that the patent specification stated that “communications are said to be transparent because the client . . . does not have to run extra procedures or modify the network source code.” NPS’ paraphrase misstates the patent language. The full section cited by NPS stated:

The apparatus in accordance with the invention is, however, configured to provide a transparent interface between the interconnected networks so that clients on either network can run standard network service applications transparently without extra procedures, or modifications to accomplish communications across the secure gateway.

(Col. 6:28–34.) NPS’ interpretation of this passage improperly turns the last 12 words into an explanation of the word “transparently.” The passage did not state that the network service applications were transparent *because* they were run without extra procedures or modifications. Rather, transparency was one of three distinct characteristics of network service applications in the patented invention. Further, Fortinet’s proposed construction allows this passage to be read without rendering the last 12 words in the sentence redundant.

*Third*, NPS points out that during reexamination, Fortinet’s proposed definition of transparently was something more akin to NPS’ current construction, and that Fortinet has since changed its tune. At the time, Fortinet was pushing to define transparency as not requiring a user login. This is similar to NPS’ current proposal, which references “extra procedures” that NPS argues applied to user logins.

Despite this similarity, Fortinet’s prior position is materially different from NPS’ current construction. NPS’s construction not only references extra procedures, it also references “modifications.” Fortinet’s prior position and NPS’ current position are thus not directly comparable. The fact that Fortinet previously relied on a materially different construction casts doubt over Fortinet’s current position, but it does not help NPS in equal measure. Nor is there any basis to deem Fortinet estopped from advancing a different position in this proceeding.

At oral argument, NPS’ counsel stated they would accept the same definition of transparently that Fortinet advanced during reexamination. However, the record in this action

does not contain adequate briefing on that construction. Based on the available evidence, this order tentatively adopts Fortinet’s proposal for “transparently”: “appearing to the initiator to be one direct communications session.” The parties are invited to address the issue of Fortinet’s contention at reexamination in their critiques of this preliminary claim construction order.

**F. “Accepting at the gateway”**

The parties dispute the term “accepting at the gateway.” The parties’ proposed constructions are provided below:

NPS’ PROPOSED CONSTRUCTION	FORTINET’S PROPOSED CONSTRUCTION
Allowing received packets to be processed by the gateway even though the packets designate an IP destination address other than that of the gateway.	Retaining for further evaluation and processing at the application level network gateway.
or (at oral argument):	
Allowing received packets to be processed by a gateway with application level security and data screening capability even though the packets designate an IP destination address other than that of the gateway.	

This order holds that the ordinary meaning of the term to a POSA in 1994 should govern. Although the parties do not recognize their common ground, they agree that “accepting at the gateway” meant “receiving” packets at the gateway instead of rejecting them. This is simply a plain meaning construction of the term, and it is supported in particular by Figure 6 in the patent, which showed the first packet processing step on a UNIX embodiment as “receive data packet.” Moreover, at oral argument both parties agreed that a plain meaning construction would be acceptable to them.

This order agrees that a plain language construction charts a better course. Both parties’ constructions attempt to read in additional limitations to the claim term, but neither provides an adequate justification for doing so. Fortinet’s construction adds the additional element of “retaining for further evaluation.” It is clear from the claim language and from Figure 6 of the patent, however, that the disputed term only referred to the first step in the packet processing

1 process, and not to retention after receipt. Fortinet's construction is also ambiguous because it is  
2 not clear whether "retaining" refers to receipt at the application level network gateway, or receipt  
3 at the gateway before being retained for processing at the application level.

4 NPS attempts to include a limitation based on the IP destination address of the packet.  
5 NPS does not explain why this limitation should be read into the claim, and did not address this  
6 issue at oral argument. The closest NPS comes to justifying this position is its assertion that  
7 language in the patent supports the interpretation that the gateway would accept packets  
8 regardless of their IP address. This is equivalent to arguing that accepting packets regardless of  
9 IP destination address was an *implied result* of the other claims. It does not justify adding an  
10 additional concept to the definition of the claim term.

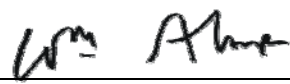
11 Neither party has justified their constructions, and this order shall hold the parties to their  
12 common ground at oral argument: the plain meaning of the term to a POSA in 1994 shall  
13 govern.

#### 14 CONCLUSION

15 The constructions set forth above will apply in this action. The Court reserves the  
16 authority, on its own motion, to modify these constructions if further evidence warrants such a  
17 modification (but counsel may not move to reconsider them). Additionally, by **NOON ON**  
18 **JANUARY 2**, each side may file a five-page critique (double-spaced, 12-point Times New Roman  
19 font, no footnotes, and no attachments) limited to points of critical concern. This is an  
20 opportunity for the parties to focus solely on their most cogent critique, not to rehash every point  
21 made in the briefs and at the hearing. No replies, please.

22  
23 **IT IS SO ORDERED.**

24  
25 Dated: December 21, 2012.

  
\_\_\_\_\_  
WILLIAM ALSUP  
UNITED STATES DISTRICT JUDGE